

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

APR 26 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST LOUIS

In the Matter of the Search of

INFORMATION ASSOCIATED WITH EMAIL
ACCOUNTS (1) rnbrwar@aol.com and (2)
shartals@aol.com THAT IS STORED AT PREMISES
CONTROLLED BY OATH, INC. (See Attachment A)

Case No. 4:19 MJ 5190 NAB

APPLICATION FOR A SEARCH WARRANT

I, Marla Vanderbunt, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

INFORMATION ASSOCIATED WITH EMAIL ACCOUNTS (1) rnbrwar@aol.com and (2) shartals@aol.com THAT IS STORED AT PREMISES
CONTROLLED BY OATH, INC. (See Attachment A)

located in the EASTERN District of VIRGINIA, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. Section 1030

Computer Intrusion

18 U.S.C. Section 1343

Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

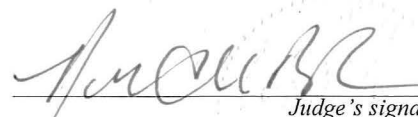
Marla Vanderbunt

Special Agent, Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: April 26, 2019



Judge's signature

City and state: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge

Printed name and title

AUSA: Kyle T. Bateman

FILED

APR 26 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST LOUIS

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
ACCOUNTS: shartals@aol.com and
rnbrawar@aol.com

Case No. 4:19 MJ 5190 NAB

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Marla Vanderbunt, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts and a domain that are stored at premises controlled by Oath Inc. ("Oath"), an e-mail provider headquartered at 22000 AOL Way, Dulles, VA 20166. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since April 2006. I am currently assigned to the St. Louis Field Office of the FBI, assigned to full-time investigations of computer crimes with specific responsibility for criminal computer intrusions. Prior to my current assignment, from September 2006 to November 2014, I was assigned to a white collar squad specializing in health care fraud investigations. Through my

training and experience as a special agent, I am familiar with investigations involving individuals who execute computer intrusions, including the execution of search warrants on computers and email accounts.

3. I have also participated in the execution of federal search warrants, a number of which involved Computer Intrusion as detailed by Section 1030 of Title 18, United States Code. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030 (computer intrusion) and 1343 (wire fraud), and conspiracy to commit such offenses, have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

**BACKGROUND INFORMATION REGARDING COMPUTERS,
THE INTERNET, AND E-MAIL:**

7. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

a. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the Internet to share information.

c. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless, and numerous other methods.

d. Computers connected to the Internet are identified by addresses. Internet addresses take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can identify a physical location and a computer connection.

8. Electronic mail (or "email") is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

PROBABLE CAUSE

9. As part of an ongoing investigation, I learned that in June 2018, Victim 1, a large corporation in St. Louis, Missouri, within the Eastern District of Missouri, identified medical claim payments issued through electronic fund transfers (EFTs) being redirected to suspicious bank accounts. Through Victim 1's initial stages of an internal investigation, the venue of attack appears to be a vulnerability in the external EFT payment process for Victim 2, which is Victim 1's external vendor for electronic payment processing.

10. Victim 1 contracts with Victim 2 to facilitate payments between Victim 1 and medical providers. Victim 2's role is to facilitate monetary payment between correspondent payers and medical providers, such as hospitals, medical clinics and pharmacies. Victim 2 facilitates payment through a provider portal, where the medical providers register for new accounts using their tax ID, national provider ID and zip code. This information is publically available. Once an account is established with Victim 2, the clients of Victim 2 can then login to Victim 2's portal with a user account registration code. Once logged into Victim 2's portal, a client would have visibility of all remittance claims submitted by the medical provider.

11. Between January 2018 and May 2018, Unknown Subjects (UNSUBs) fraudulently used the tax ID, national provider ID, and zip code of medical providers to create secondary medical provider user accounts with different email addresses. Once the UNSUBs had access to Victim 2's portal they had visibility to actual user accounts, to include visibility of registration codes held by the provider. The UNSUBs looked for registration codes that were not being used and in turn added banking data to the unregistered codes. The UNSUBs looked for the unregistered codes of the medical providers that accepted paper payments and did not accept EFT's. The UNSUBs changed the paper payments into EFT for these medical providers. This caused the victim funds to be paid directly to the UNSUBs accounts instead of the medical providers' actual accounts.

12. In my investigation, I have learned that Victim 1 has identified approximately 600 fraudulent transactions with an approximate loss of \$5 million.

Fraudulent Payments Made to and from Delia Garcia and Elizabeth Fischer

13. Delia Garcia ("Garcia") is an individual who holds a bank account ending in #5729 at East Boston Savings Bank (the "Garcia Account") that received some of the fraudulent payments from Victim 1 as described above. Specifically, on June 4, 2018, the Garcia Account received an ACH transfer in the amount of \$54,811.68 from Victim 1.

14. On June 5, 2018, there were two electronic transfers to other accounts at East Boston Savings Bank, including \$8,857 to an account ending in #6466 and \$15,000 to an account ending in #6980. On the same day, Garcia purchased an Official Check in the amount of \$30,150 made payable to "Daiselk, LLC."

15. According to public records from California Secretary of State, Daiselk, LLC, (“Daiselk”) is a business entity formed on February 6, 2018. Daiselk is associated with address 8631 Folsom Blvd, Sacramento, California, and Elizabeth Fisher (“Fisher”) is listed as a manager, member and Chief Executive Officer for Daiselk.

16. On March 7, 2019, Agents interviewed Fisher. Fisher stated she met an individual by the name of “Leo Andre” on an online dating service known as Zooks in November 2016. According to Fisher, in or about February 2018, Andre told Fischer that he was using her name to form Daiselk in the State of California. Andre then instructed Fisher to open J.P. Morgan Chase bank account ending in #1317 in the name of Daiselk (the “Daiselk Account”). Fisher subsequently opened bank accounts in the name of Daiselk at BBVA, Bank of America, Chase and Wells Fargo. Fisher stated that she sent money to Andre, who told her that he was traveling between England and South Africa. Fisher stated that she gave the account login credentials for the bank accounts associated with Daiselk to Andre for direct access to move money to and from the accounts.

17. Records received from J.P. Morgan Chase Bank on the Daiselk Account confirm that the signor on the account is Elizabeth Fisher at address 8631 Folsom Blvd, Sacramento, CA.

Additional Fraudulent Payments to the Daiselk Account

18. In or about September 2018, and thereafter, US Business 1 was attempting to initiate a wire transfer to US Business 2 for services rendered.

19. At some point during email communications between the parties related to the wire transfer, legitimate email addresses for employees with US Business 2 (shartels@aol.com and mnbrower@aol.com) were changed to fraudulent email addresses (shartals@aol.com and

rnbravar@aol.com). Following the change, the fraudulent email addresses directed US Business 1 to wire funds to the Daiselk Account instead of US Business 2's actual bank account.

20. In or about September 2018, as a result of the direction in email messages from the fraudulent email addresses, US Business 1 sent a wire transfer in the amount of \$288,751.59 to the Daiselk Account.

21. A review of the Daiselk Account showed a wire deposit of \$288,751.59 on September 25, 2018. Fisher initiated several withdrawals from the Daiselk Account, including the following:

- a. On September 25, 2018, a cashier's check in the amount of \$100,000 was made payable to Daiselk LLC, which was thereafter deposited it into Daiselk's Wells Fargo account; another cashier's check in the amount of \$9,500 was made payable to Oki Kacely Bius; and another cashier's check in the amount of \$9,500 was made payable to Oki Kacely Pius.
- b. On September 26, 2018, a cashier's checks in the amount of \$9,500 was made payable to Franklin Karen Obioma; another cashier's check in the amount of \$20,000 was made payable to Nchekwube C. Aroh; and another cashier's check in the amount of \$16,780 was made payable to Olushola Oluyeba.
- c. On September 27, 2018, an international wire transfer in the amount of \$45,000 was sent to Firststrand Bank located in Johannesburg, South Africa.
- d. On September 28, 2018, another international wire transfer in the amount of \$45,000 was sent to Firststrand Bank located in Johannesburg, South Africa.
- e. On October 1, 2018, an international wire transfer in the amount of \$13,000 was sent to Nedbank Ltd located in Johannesburg, South Africa.

22. In January 2019, Agents interviewed personnel with US Business 2 in which they advised that they did not provide the instructions to wire funds to the Daiselk Account. US Business 2 personnel advised that the Daiselk Account is not associated with them and that US Business 2 never received any expected funds from US Business 1. US Business 2 personnel further advised that they did not know that email communications with rnbrawar@aol.com and shartals@aol.com took place with US Business 1 until after the fraudulent wire transfer took place. US Business 2 personnel advised that email accounts rnbrawar@aol.com and shartals@aol.com are not email accounts associated with US Business 2. US Business 2 email accounts shartels@aol.com and rnbrawer@aol.com are known employees at US Business 2 and were known email accounts to exchange email communications with US Business 1.

23. Records received from Oath Inc. on email account rnbrawar@aol.com showed the account was created on September 20, 2018 at 18:15:29 using IP address 105.4.2.51 and phone number +27610622510. This account contained additional login data from IP addresses 105.0.2.136 and 105.4.7.95 in October 2018. The international phone number country code +27 resides to South Africa. The three above IP addresses starting with 105 also reside to Johannesburg, South Africa.

24. Records received from Oath Inc. on email account shartals@aol.com showed the account was created on September 20, 2018 at 18:26:18 using IP address 105.4.2.51 and phone number +27610622510. This account contained additional login data from IP addresses 105.4.7.95 (Johannesburg, South Africa) and 41.246.185.219 (Pretoria, South Africa). The international phone number country code +27 resides to South Africa.

25. Email accounts rnbrwar@aol.com and shartals@aol.com were created on the same day within in approximately eleven minutes of each other.

26. US Business 2 stated they do not have business relations in South Africa to include using any phone numbers and/or IP addresses associated with South Africa.

27. In conclusion, the Daiselk Account received fraudulent funds from Victim 1 and fraudulent funds from US Business 1. Elizabeth Fischer stated she met an individual online that claimed to travel to South Africa, and subscriber information associated with email addresses rnbrwar@aol.com and shartals@aol.com contained South African login data and phone numbers. The fraudulent wire transfer sent by US Business 1 to the Daiselk Account was initiated through email accounts rnbrwar@aol.com and shartals@aol.com.

BACKGROUND CONCERNING EMAIL

28. In my training and experience, I have learned that Oath provides a variety of on-line services, including electronic mail ("email") access, to the public. Subscribers obtain an account by registering with Oath. During the registration process, email providers ask subscribers to provide basic personal information. Therefore, the computers of Oath are likely to contain stored electronic communications (including retrieved and unretrieved email for Oath subscribers) and information concerning subscribers and their use of Oath services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. A Oath subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Oath. In my training and

experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

30. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

31. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

32. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account

owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

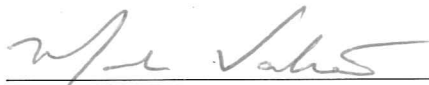
34. Based on the aforementioned factual information, I respectfully request that the Court issue the proposed search warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for content) and 18 U.S.C. § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41. Because the warrant will be served on Oath, which will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

35. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Marla Vanderbunt
Special Agent
FEDERAL BUREAU OF INVESTIGATION

SUBSCRIBED and SWORN to before me on April 25, 2019



The Honorable ~~Nanette A. Baker~~
United States Magistrate Judge

Nannette A. Baker

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email accounts (1) rnbrewar@aol.com and (2) shartals@aol.com that are stored at premises controlled by Oath Inc., a company that accepts service of legal process at lawenforcement@teamaol.com.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Oath Inc. (Oath) (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. The contents of all instant messages associated with the account, including stored or preserved copies of instant message, the date and time at which each instant message was sent/received;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. The types of service utilized;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. Any and all cookies associated with or used by any computer or web browser associated with each account, including the IP addresses, dates, and times associated with the recognition of any such cookie. Subscriber information for other accounts accessed by computers or browsers using the same cookie as the account.

g. Any information identifying the device or devices used to access each account, including a device serial number, a GUID or Global Unique Identifier, a phone number, Media Access Control (“MAC”) address, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), International Mobile Equipment Identities (“IMEI”), or ID for advertisers (“IDFA”), and any other information regarding the types of devices used to access each account.

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1030 and 1343, those violations involving the unknown individual and occurring on/after December 1, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Communications between Oath accounts rnbrawar@aol.com and shartals@aol.com, and other email addresses to identify co-conspirators and victims;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation; and
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Oath Inc. and my official title is _____. I am a custodian of records for Oath Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Oath Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Oath Inc.; and
- c. such records were made by Oath Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature